CLAIMS:

1. A method in a data processing system for maintaining secure user private keys in a non-secure storage device, said method comprising the steps of:

establishing a master key pair for said system, said master key pair including a master private key and a master public key;

storing said master key pair in a protected storage device;

establishing a unique user key pair for a user, said user key pair including a user private key and a user public key;

encrypting said user private key utilizing said master public key; and

storing said encrypted user private key in said non-secure storage device, wherein said encrypted user private key is secure while stored in said non-secure storage device.

2. The method according to claim 1, further comprising the steps of:

establishing an encryption device having an encryption engine and said protected storage device; and

said protected storage device being accessible only through said encryption engine.

3. The method according to claim 2, further comprising the step of said encryption engine encrypting said user private key utilizing said master public key stored in said protected storage device.

4. The method according to claim 3, further comprising the steps of:

an application generating a message to transmit to a recipient;

said encryption engine decrypting said user private key utilizing said master private key;

said encryption engine encrypting said message utilizing said decrypted user private key and a recipient's public key; and

said system transmitting said encrypted message to said recipient.

5. The method according to claim 4, wherein the step of establishing a user key pair further comprises the step of associating said user key pair with an application.

6. The method according to claim 5, further comprising the steps of:

establishing a certificate, said certificate being associated with said application, said user private key, and said user;

in response to said user attempting to access said application utilizing said certificate, said encryption engine utilizing said certificate to determine a location within said non-secure storage device for said user private key associated with said certificate;

said encryption engine decrypting said user private key; and

said encryption engine utilizing said decrypted user private key to encrypt messages transmitted by said application.

7. The method according to claim 6, wherein said step of storing said user private key in said non-secure storage further comprises the step of storing said user private key in a hard drive.

8. The method according to claim 7, further comprising the step of said user key pair being capable of being utilized only in said data processing system wherein said user key pair is established, wherein said user key pair is not capable of being utilized in a second data processing system.

9. A data processing system for maintaining secure user private keys in a non-secure storage device, comprising:

an encryption device included within said system for establishing a master key pair for said system, said master key pair including a master private key and a master public key;

a protected storage device for storing said master key pair;

said encryption device executing code for establishing a unique user key pair for a user, said user key pair including a user private key and a user public key;

said encryption device executing code for encrypting said user private key utilizing said master public key; and

said non-secure storage device for storing said encrypted user private key, wherein said encrypted user private key is secure while stored in said non-secure storage device.

10. The system according to claim 9, further comprising:

said encryption device including an encryption engine and said protected storage device; and

said protected storage device capable of being accessed only through said encryption engine.

Sub B2

11. The system according to claim 10, further comprising said encryption engine executing code for encrypting said user private key utilizing said master public key stored in said protected storage device.

12. The system according to claim 11, further comprising:

an application capable of generating a message to transmit to a recipient;

said encryption engine executing code for decrypting said user private key utilizing said master private key;

said encryption engine executing code for encrypting said message utilizing said decrypted user private key and a recipient's public key; and

said system transmitting said encrypted message to said recipient.

13. The system according to claim 12, further comprising said system executing code for associating said user key pair with an application.

14. The system according to claim 13, further comprising:

said system executing code for establishing a certificate, said certificate being associated with said application, said user private key, and said user;

in response to said user attempting to access said application utilizing said certificate, said encryption engine executing code utilizing said certificate for determining a location within said non-secure storage device for said user private key associated with said certificate;

said encryption engine executing code for decrypting said user private key pair; and

said encryption engine capable of utilizing said decrypted user private key to encrypt messages transmitted by said application.

15. The system according to claim 14, further comprising said system executing code for storing said user private key in a hard drive.

16. The system according to claim 15, further comprising said user key pair being capable of being utilized only in said data processing system wherein said user key pair is established, wherein said user key pair is not capable of being utilized in a second data processing system.

17. A data processing system for maintaining secure user private keys in a non-secure hard drive, comprising:

an encryption device including an encryption engine and a protected storage device for establishing a master key pair for said system, said master key pair including a master private key and a master public key, said protected storage device for storing said master key pair, said protected storage device capable of being accessed only through said encryption engine;

said encryption device executing code for establishing a unique user key pair for a user, said user key pair including a user private key and a user public key, said user key pair being capable of being utilized only in said data processing system wherein said user key pair is established, wherein said user key pair is not capable of being utilized in a second data processing system;

said system executing code for associating said user key pair with an application;

said encryption device executing code for encrypting said user private key utilizing said master private key stored in said protected storage device;

said non-secure hard drive for storing said encrypted user private key, wherein said encrypted user private key is secure while stored in said non-secure hard drive;

an application capable of generating a message to transmit to a recipient;

said system executing code for establishing a certificate, said certificate being associated with said application, said user private key, and said user;

storing said certificate in said non-secure hard drive;

in response to said user attempting to access said application utilizing said certificate, said encryption engine executing code utilizing said certificate for determining a location within said non-secure hard drive for said user private key associated with said certificate;

said encryption engine executing code for decrypting said user private key;

said encryption engine capable of utilizing said decrypted user private key to encrypt messages transmitted by said application; and

said system transmitting said encrypted message to said recipient.